State of Utah

Information Technology Unauthorized Access Warning Banner Policy

Purpose.

To provide guidance for the use of the Unauthorized Access Warning Banner on state computer systems.

Application.

A. All state agencies of the executive branch of government shall comply with this policy, which shall apply to all computer systems.

B. As computer systems and the information therein have varying levels of sensitivity and risk, they must comply with different levels of security requirements. This policy provides the minimum requirements for the use of Unauthorized Access Warning Banners. State agencies have the option, and are encouraged, to adopt a more stringent Unauthorized Access Warning Banner to meet the specific security requirements for their individual computer systems.

C. The requirements in this policy are specifically addressed to those who control access to the state's computer systems and the information therein. This would include managers of computer systems, computer network and computer system administrators, information/data security administrators, etc.

Definitions.

A. **Computer System** - An all-inclusive term referring to any computer, computer network, computer device, etc.

B. **Unauthorized Access Warning Banner** - A message displayed on a computer monitor, informing the potential user of access restrictions to the computer system.

C. **Login Process** - A process used by a person to obtain access to a computer system. This process consists of Identification and Authentication processes. The Identification process takes place when the person attempting access will identify them with a unique user/account name. The Authentication process takes place when the person attempting access will provide information (i.e., password, biometric information or information contained on a smartcard) that is unique to that person.

Unauthorized Access Warning Banner Procedures.

A. The Unauthorized Access Warning Banner provides the computer system administrator with the means to notify potential users of access restrictions on the computer system. It is one of the passive tools to be used by computer systems administrators in their computer security programs.

Use of the Unauthorized Access Warning Banner is important in establishing □due diligence□ in the protection of the computer system and the information therein.

B. The Unauthorized Access Warning Banner provides the user with a notification that the computer system about to be accessed has access restrictions. It is the electronic equivalent of a □No Trespassing□ sign.

C. The Unauthorized Access Warning Banner shall be displayed every time a user accesses a computer system.

1. The Unauthorized Access Warning Banner must inform the user of the computer system before access is attempted, giving the user the opportunity to avoid violating any access restrictions.

2. When access to a computer system is controlled by a login process, the Unauthorized Access Warning Banner will be displayed before the user can complete the login process, and specifically before a user starts the Authentication process. If possible, the Warning Banner should appear prominently on the same visual screen or display as the login instructions.

3. When access to a computer system is not controlled by a login process, the Unauthorized Access Warning Banner will be displayed before a user enters the system.

    a. Computer systems attached to a network and computer systems in a Single Sign-On environment will often allow access without a login process. However, where entry into the network or the Single Sign-On environment requires a login process, the Unauthorized Access Warning Banner will be displayed before the user can complete the login process (see above).

    b. Stand-alone computer systems (i.e., desktop computers, laptop computers, etc.) typically do not have a login process. These computers will display the Unauthorized Access Warning Banner as part of the start-up process. If the Warning Banner does not appear on the same screen or display as the login process, it must appear immediately before and require an acknowledgment of the warning (i.e., in the form of an icon or on-screen button stating OK or I Accept). If an Unauthorized Access Warning Banner cannot be added to the start-up process, an Unauthorized Access Warning Banner sticker will be prominently displayed on the stand-alone computer system.

D. If an Unauthorized Access Warning Banner cannot be displayed and notify a potential user of access restrictions, the circumstances will be documented, approved and signed by the organizational manager.

E. The failure to comply with this policy or to place an Unauthorized Access Warning Banner in accordance with this policy shall not be deemed an authorization to any person to access the computer system if the person is not otherwise authorized by the State

F. Following is the recommended Unauthorized Access Warning Banner:

WARNING

THIS SYSTEM IS RESTRICTED TO AUTHORIZED USERS FOR OFFICIAL USE ONLY AND SHALL BE IN ACCORDANCE WITH THE ACCEPTABLE USE POLICY. USE OF THIS SYSTEM IS SUBJECT TO MONITORING. UNAUTHORIZED ACCESS IS A VIOLATION OF APPLICABLE LAWS AND REGULATIONS. VIOLATORS WILL BE PROSECUTED.